UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,645	01/24/2004	Ron Khormaei	100201951-1	9156

22879 7590 04/30/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
04/30/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
jessica.l.fusek@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/764,645	KHORMAEI ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 2/17/09.

2. Claims 1-25 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/21/09 has been entered.

Response to Arguments

4. Applicant's arguments with respect to the prior art rejections have been fully considered but they are not persuasive.

5. Applicant argues in substance that the Tresser prior art does not disclose the new limitations of the claimed invention. However, as outlined below, the new limitations are obvious in view of Tresser. See rejections below.

6. Applicant's remaining arguments are derivative of those discussed above.

Claim Rejections - 35 USC § 101

7. Claims 1-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1, 2 and 4-12 define a method to generate an authentication key for an electronic document file representative of a document, including a providing step and a submitting step; and a method of authenticating an electronic document file representative of document, including a submitting step and a using step. However, none of these steps require a specific machine; and there is no transformation of an article or representation of an article (the method only discloses modification of "information" or "digital data") See In re Bilski, 2007-1130 at 15, ("At present, however, and certainly for the present case, we see no need for such a departure and reaffirm that the machine-or-transformation test, properly applied, is the governing test for determining patent eligibility of a process under § 101." The Court also points to the Abele case where a dependent process claim was determined to be statutory under 101 but not the independent claim; the dependent claim was a sufficiently specific transformation because it changed "raw data into a particular visual depiction of a physical object on a display"; the transformed object must be "physical objects or substances" or "representative of physical objects or substances," id. at 30 and 32).

8. As for claim 3, although claim 3 discloses displaying the digital halftone file on a user display to provide a visible copy of the document and the authentication key, this feature constitutes extra-solution activity that does not provide any meaningful limits to the scope of the claimed invention. The method defined by independent claims 1 and 7 are methods of generating an authentication key for an electronic document file.

Display of the generated authentication key is not a critical step of a method to generate a key value.

Claim Rejections - 35 USC § 103

9. Claims 1-11 and 14-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tresser et al. USPN 6,804,373 (hereinafter Tresser).

10. As per claims 1-6, Tresser discloses a method of generating an authentication key for an electronic document file representative of a document, the method comprising:

a. providing the electronic document file as an initial digital file; (col. 8:56-9:3)

b. submitting the initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file; and (9:4-7 and lines 40-44: I(i,j) is converted to I'(h,v) by averaging gray levels over rectangles of a grid covering image I; I'(h,v) is converted to M(h,v) by a halftoning process)

c. submitting the digital halftone file to a predetermined mathematical process to thereby generate the authentication key; (9:7-32; information from M is signed)

d. printing the digital halftone file to provide a tangible copy of the document, and printing with the tangible copy of the document a visible representation of the authentication key; (9:66-10:5; a scannable signature is embedded in the image)

e. displaying the digital halftone file on a user display to provide a visible copy of the document and the authentication key; (10:61-64)

f. wherein the halftoning process is based, at least in part, on an error diffusion halftoning algorithm; (5:30-31 and lines 41-44)

g. wherein the halftoning process is based, at least in part, on one of a matrix-based halftoning algorithm, a pattern-based halftoning algorithm, or an ordered-dither halftoning algorithm; (5:15-41; 9:4-7) and

h. wherein the predetermined mathematical process is a summation process. (6:6-25)

11. Although the embodiment disclosed by Tresser discloses the invention in the context of a black and white printing system, Tresser expressly discloses that the invention is applicable to color and multitone printers. Col. 6:49-53. On col. 9, lines 8-19, Tresser discloses:

> At 340, matrix M is interpreted as a data stream, and optionally (selectively) cut into a plurality of pieces (some of which can overlap). These pieces can, for instance, form blocks, not necessarily all of the same size (the blocks may have the same size or may have a different size depending upon the ease versus generality desired by the designer), that cover M, or can correspond to intertwined parts of M. Some of the pieces may be processed in an image compression engine at 351, one example of which will be described in more detail below. Other pieces may be processed at 352 by a digital signature scheme such as for instance the RSA scheme.

12. In this case, matrix M is an output of a half-toning procedure for a black and white printer. For an embodiment constituting color or multitone printers, a data

structure (M) analogous to the matrix M stores the bit data resulting from the halftone procedure to process the multiple planes of an image for a color or multitone printer. In this case, the digital signature scheme would necessarily apply to a plurality of pieces of the resulting data structure (M). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different color ink drops, and wherein the mathematical process includes mathematically combining the multiplane bitmap to create the authentication key. One would be motivated to do so to authenticate a color image as taught by Tresser. Col. 6:49-53. The aforementioned cover the limitations of claims 1-6.

13. As per claims 7-11, Tresser discloses a method of authenticating an electronic document file representative of a document, the method comprising:

i. receiving the electronic document file as an initial received digital file; submitting the initial received digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file defined by a plurality of discrete digital values; submitting the digital halftone file to a mathematical process involving each of the plurality of discrete digital values in the digital halftone file, thereby produce a receiver-generated authentication key for the initial received digital file; and using the receiver-generated authentication key to verify the authenticity of the initial received digital file relative to the electronic document file; wherein the step of using the receiver-

generated authentication key comprises: receiving a sender-generated authentication key for the electronic document file; and comparing the sender-generated authentication key to the receiver-generated authentication key; and accepting the authenticity of the initial received digital file relative to the electronic document file, when the sender-generated and the receiver-generated authentication keys are identical; (col. 6:15-26, RSA signatures are generated using a hash of the digital data; 9:63-10:48, especially 10:36-41; the inverse of the signature is a compressed version of N'; embedded matrix M is necessarily transformed to compressed version of half tone N, whereby a match authenticates the document)

j. wherein the halftoning process is based, at least in part, on an error diffusion halftoning algorithm; (5:30-31 and lines 41-44)

k. wherein the halftoning process is based, at least in part, on one of a matrix-based halftoning algorithm, a pattern-based halftoning algorithm, or an ordered-dither halftoning algorithm; and (5:15-41; 9:4-7)

l. wherein the predetermined mathematical process is a summation process. (6:6-25)

14. Although the embodiment disclosed by Tresser discloses the invention in the context of a black and white printing system, Tresser expressly discloses that the invention is applicable to color and multitone printers. Col. 6:49-53. On col. 9, lines 8-19, Tresser discloses:

> At 340, matrix M is interpreted as a data stream, and optionally (selectively) cut into a plurality of pieces (some of which can overlap). These pieces can, for instance, form

> blocks, not necessarily all of the same size (the blocks may have the same size or may have a different size depending upon the ease versus generality desired by the designer), that cover M, or can correspond to intertwined parts of M. Some of the pieces may be processed in an image compression engine at 351, one example of which will be described in more detail below. Other pieces may be processed at 352 by a digital signature scheme such as for instance the RSA scheme.

15. In this case, matrix M is an output of a half-toning procedure for a black and white printer. For an embodiment constituting color or multitone printers, a data structure (M) analogous to the matrix M stores the bit data resulting from the halftone procedure to process the multiple planes of an image for a color or multitone printer. In this case, the digital signature scheme would necessarily apply to a plurality of pieces of the resulting data structure (M). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different color ink drops, and wherein the mathematical process includes mathematically combining the multiplane bitmap to create the authentication key. One would be motivated to do so to authenticate a color image as taught by Tresser. Col. 6:49-53. The aforementioned cover the limitations of claims 7-11.

16. As per claim 14, Tresser discloses a system to generate an authentication key for an electronic document file representative of a document, the system comprising: a processor; and a computer readable memory device readable by the processor (fig. 7 and related text), the computer readable memory device containing a series of computer executable steps configured to cause the processor to: retrieve a copy of the electronic document file as an initial digital file (col. 8:56-9:3); submit the initial digital file

without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file (9:4-7 and lines 40-44); submit the digital halftone file to a predetermined mathematical process to thereby generate the authentication key (9:17-19 and lines 25-32); and store a copy of the authentication key in the computer readable memory device. (fig. 3, reference no. 380; 10:53-54)

17. Although the embodiment disclosed by Tresser discloses the invention in the context of a black and white printing system, Tresser expressly discloses that the invention is applicable to color and multitone printers. Col. 6:49-53. On col. 9, lines 8-19, Tresser discloses:

> At 340, matrix M is interpreted as a data stream, and optionally (selectively) cut into a plurality of pieces (some of which can overlap). These pieces can, for instance, form blocks, not necessarily all of the same size (the blocks may have the same size or may have a different size depending upon the ease versus generality desired by the designer), that cover M, or can correspond to intertwined parts of M. Some of the pieces may be processed in an image compression engine at 351, one example of which will be described in more detail below. Other pieces may be processed at 352 by a digital signature scheme such as for instance the RSA scheme.

18. In this case, matrix M is an output of a half-toning procedure for a black and white printer. For an embodiment constituting color or multitone printers, a data structure (M) analogous to the matrix M stores the bit data resulting from the halftone procedure to process the multiple planes of an image for a color or multitone printer. In this case, the digital signature scheme would necessarily apply to a plurality of pieces of the resulting data structure (M). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different color ink drops, and wherein the mathematical process includes mathematically combining the

multiplane bitmap to create the authentication key. One would be motivated to do so to authenticate a color image as taught by Tresser. Col. 6:49-53.

19. As per claim 15, the rejection of claim 14 under 35 USC 103(a) as being unpatentable over Tresser is incorporated herein. In addition, Tresser further discloses wherein the processor and the computer readable memory device are resident within a document printing device. (col. 1:10-12; fig. 7, reference no. 739)

20. As per claim 16, the rejection of claim 15 under 35 USC 103(a) as being unpatentable over Tresser is incorporated herein. In addition, Tresser further discloses wherein the series of computer executable steps are further configured to cause the processor to print a tangible copy of the halftone image file as the document, and to include the authentication key on the tangible copy of the halftone image file. (Col. 9:66-10:5)

21. As per claim 17, the rejection of claim 14 under 35 USC 103(a) as being unpatentable over Tresser is incorporated herein. In addition, Tresser further discloses wherein the computer readable memory is configured to store, at least temporarily, a copy of the electronic document file as the initial digital document file. (fig. 3, reference no. 380; 10:53-54)

22. As per claim 18, the rejection of claim 15 under 35 USC 103(a) as being unpatentable over Tresser is incorporated herein. In addition, Tresser discloses the system further comprising a user display, and wherein the series of computer executable steps are further configured to cause the processor to display the authentication key on the user display. (Col. 10:61-64)

Claim Rejections - 35 USC § 103

23. Claims 12 and 13 are rejected under 35 USC 103(a) as being unpatentable over Tresser in view of Linsker et al. USPN 5,598,473 (hereinafter Linsker).

24. As per claims 12 and 13, the rejections of claims 9 and 10 as being unpatentable over Tresser are incorporated herein. Tresser does not disclose wherein the electronic document file is received from a sender via a network and wherein the sender authentication key is received via one of telephone or facsimile. Linsker discloses using an authentication key to verify the integrity of a fax transmission from a sender to a receiver. The authentication key is based on a digest of a digital document and signature of the digest, which is appended to the document and faxed to the receiver. The receiver recovers the first digest from the signature then performs an operation on the digital document to create a second digest, wherein a match between the first and second digest shows that the document is authentic. Col. 6:33-8:15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the electronic document file of Tresser to be received from a sender via a network and

wherein the sender authentication key is received via one of telephone or facsimile. One would be motivated to do so to ensure the authenticity of documents transmitted via fax using an authentication key derived from halftoning digital information, a process that provides the requisite security, whether or not the document was scanned properly. (Linsker, 1:43-55; Tresser, 3:49-55) The aforementioned cover the limitations of claims 12 and 13.

25. Claims 19, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tresser in view of Brundage et al. US Patent Application Publication No. 20040181671 (hereinafter Brundage).

26. As per claim 19, Tresser discloses a system for authenticating an electronic document file representative of a document, the system comprising: a processor; a computer readable memory device readable by the processor (fig. 7 and related text) and configured to receive the electronic document file as an initial received digital file; the computer readable memory device containing a series of computer executable steps configured to cause the processor to: store the initial received digital file in the computer readable memory device; submit the initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file defined by a plurality of discrete digital values; submit the digital halftone file to a predetermined mathematical process involving each of the plurality of discrete digital values in the digital halftone file to thereby produce a receiver-generated

authentication key for the initial received digital file. (col. 6:15-26, RSA signatures are generated using a hash of the digital data; col. 9:63-10:48, especially 10:36-41; the inverse of the signature is a compressed version of N'; embedded matrix M is transformed to compressed version of half tone N, a match authenticates the document)

27. Although the embodiment disclosed by Tresser discloses the invention in the context of a black and white printing system, Tresser expressly discloses that the invention is applicable to color and multitone printers. Col. 6:49-53. On col. 9, lines 8-19, Tresser discloses:

> At 340, matrix M is interpreted as a data stream, and optionally (selectively) cut into a plurality of pieces (some of which can overlap). These pieces can, for instance, form blocks, not necessarily all of the same size (the blocks may have the same size or may have a different size depending upon the ease versus generality desired by the designer), that cover M, or can correspond to intertwined parts of M. Some of the pieces may be processed in an image compression engine at 351, one example of which will be described in more detail below. Other pieces may be processed at 352 by a digital signature scheme such as for instance the RSA scheme.

28. In this case, matrix M is an output of a half-toning procedure for a black and white printer. For an embodiment constituting color or multitone printers, a data structure (M) analogous to the matrix M stores the bit data resulting from the halftone procedure to process the multiple planes of an image for a color or multitone printer. In this case, the digital signature scheme would necessarily apply to a plurality of pieces of the resulting data structure (M). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different color ink drops, and wherein the mathematical process includes mathematically combining the

multiplane bitmap to create the authentication key. One would be motivated to do so to authenticate a color image as taught by Tresser. Col. 6:49-53.

29. In addition, Tresser does not disclose displaying a copy of the receiver-generated authentication key on one of a printer or a user display. Brundage discloses a system for authenticating identification documents using a watermark, wherein an authenticator displays the watermark information to a user to allow an inspector or officer to visually compare the watermark information against information printed on the document. Paragraph 62. It would be obvious to one of ordinary skill in the art at the time the invention was made to display a copy of the receiver-generated authentication key on one of a printer or a user display. One would be motivated to do so to enable a human to quantify the authenticity of the document as taught by Brundage, ibid. The aforementioned cover the limitations of claim 19.

30. As per claim 22, the rejection of claim 19 under 35 USC 103(a) as being unpatentable over 35 USC 103(a) is incorporated herein. In addition, Tresser discloses wherein the processor and the computer readable memory device are resident within a document printing device. (col. 1:10-12; fig. 7, reference no. 739)

31. As per claim 23, Tresser discloses an system to authenticate an electronic document file, comprising:

m. a sender computer configured to provide the electronic document file in the form of a sender initial digital file; a sender printer configured to: receive the

sender initial digital file; submit the sender initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a first digital halftone file; submit the first digital halftone file to a predetermined mathematical process to thereby generate a sender authentication key; and display the sender authentication key to a sender; (col. 8:56-9:44; 10:61-64)

n. a receiver computer configured to receive the electronic document file from the sender as a receiver initial digital file; a receiver printer configured to: receive the receiver initial digital file; submit the receiver initial digital file without intervening transformation directly to the predetermined halftoning process, thereby to generate a second digital halftone file; submit the second digital halftone file to the predetermined mathematical process to thereby generate a receiver authentication key. (col. 9:63-10:48, especially 10:36-41; the inverse of the signature is a compressed version of N'; embedded matrix M is transformed to compressed version of half tone N, a match authenticates the document)

32. Although the embodiment disclosed by Tresser discloses the invention in the context of a black and white printing system, Tresser expressly discloses that the invention is applicable to color and multitone printers. Col. 6:49-53. On col. 9, lines 8-19, Tresser discloses:

> At 340, matrix M is interpreted as a data stream, and optionally (selectively) cut into a plurality of pieces (some of which can overlap). These pieces can, for instance, form blocks, not necessarily all of the same size (the blocks may have the same size or may have a different size depending upon the ease versus generality desired by the designer), that cover M, or can correspond to intertwined parts of M. Some of the pieces may be processed in an image compression engine at 351, one example of which will be

described in more detail below. Other pieces may be processed at 352 by a digital signature scheme such as for instance the RSA scheme.

33. In this case, matrix M is an output of a half-toning procedure for a black and white printer. For an embodiment constituting color or multitone printers, a data structure (M) analogous to the matrix M stores the bit data resulting from the halftone procedure to process the multiple planes of an image for a color or multitone printer. In this case, the digital signature scheme would necessarily apply to a plurality of pieces of the resulting data structure (M). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different color ink drops, and wherein the mathematical process includes mathematically combining the multiplane bitmap to create the authentication key. One would be motivated to do so to authenticate a color image as taught by Tresser. Col. 6:49-53.

34. In addition, Tresser does not disclose displaying a copy of the authentication key to a user via one of a printer or a user display. Brundage discloses a system for authenticating identification documents using a watermark, wherein an authenticator displays the watermark information to a user to allow an inspector or officer to visually compare the watermark information against information printed on the document. Paragraph 62. It would be obvious to one of ordinary skill in the art at the time the invention was made to display a copy of the authentication key to a user via one of a printer or a user display. One would be motivated to do so to enable a human to quantify the authenticity of the document as taught by Brundage, ibid. The aforementioned cover the limitations of claim 23.

35. Claims 20, 21, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tresser in view of Brundage and further in view of Linsker.

36. As per claims 20 and 21, the rejection of claim 19 under 35 USC 103(a) as being unpatentable over Tresser and Brundage are incorporated herein. Tresser does not disclose the system further comprising a modem configured to process the initial received digital file from a sender and communicate the initial received digital file to the computer readable memory device by way of the processor; and one of a telephone or a facsimile machine configured to receive a sender-generated authentication key for the electronic document file capable of being compared to the receiver-generated authentication key to authenticate the initial received digital file relative to the electronic document file. Linsker discloses using an authentication key to verify the integrity of a fax transmission from a sender to a receiver. The authentication key is based on a digest of a digital document and signature of the digest, which is appended to the document and faxed to the receiver. The receiver recovers the first digest from the signature then performs an operation on the digital document to create a second digest, wherein a match between the first and second digest shows that the document is authentic. Col. 6:33-8:15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the system of Tresser to further comprise a modem configured to process the initial received digital file from a sender and communicate the initial received digital file to the computer readable memory device by way of the

processor; and one of a telephone or a facsimile machine configured to receive a sender-generated authentication key for the electronic document file capable of being compared to the receiver-generated authentication key to authenticate the initial received digital file relative to the electronic document file. One would be motivated to do so to ensure the authenticity of documents transmitted via fax using an authentication key derived from halftoning digital information, a process that provides the requisite security, whether or not the document was scanned properly. (Linsker, 1:43-55; Tresser, 3:49-55) The aforementioned cover the limitations of claims 20 and 21.

37. As per claims 24 and 25, the rejection of claim 23 under 35 USC 103(a) as being unpatentable over Tresser and Brundage are incorporated herein. Tresser does not disclose the system further comprising a network connection configurable to allow the sender computer to send the sender initial digital file to the receiver computer; and a sender telephone and a receiver telephone together allowing the sender to communicate the sender authentication key to the receiver; or a sender facsimile machine and a receiver facsimile machine together allowing the sender to communicate the sender authentication key to the receiver. Linsker discloses using an authentication key to verify the integrity of a fax transmission from a sender to a receiver. The authentication key is based on a digest of a digital document and signature of the digest, which is appended to the document and faxed to the receiver. The receiver recovers the first digest from the signature then performs an operation on the digital

document to create a second digest, wherein a match between the first and second digest shows that the document is authentic. Col. 6:33-8:15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the system of Tresser to further comprise a network connection configurable to allow the sender computer to send the sender initial digital file to the receiver computer; and a sender telephone and a receiver telephone together allowing the sender to communicate the sender authentication key to the receiver; or a sender facsimile machine and a receiver facsimile machine together allowing the sender to communicate the sender authentication key to the receiver. One would be motivated to do so to ensure the authenticity of documents transmitted via fax using an authentication key derived from halftoning digital information, a process that provides the requisite security, whether or not the document was scanned properly. (Linsker, 1:43-55; Tresser, 3:49-55) The aforementioned cover the limitations of claims 24 and 25.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432